Guang-Can Guo, Guo-Ping Guo*
Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Science, Hefei, Anhui, P. P. China, 230026

Here we analyze the practical implication of the existing quantum data hiding protocol with Bell states produced with optical downconverter. We show that the uncertainty for the produce of the Bell states with spontaneous parameter down-conversion should be taken into account, as it will cause serious trouble to the hider encoding procedure. A set of extended Bell states and a generalized Bell states analyzer are proposed to describe and analyze the possible states of two photons distributing in the two paths. Then we present a method to combine the above uncertainty of Bell states preparation with spontaneous parameter down-conversion into the data hiding procedure, by encoding the secret with the set of extended Bell states. This greatly simplify the hider's encoding operations and then paves the road for the implementation of the quantum data hiding with present-day quantum optics.

PACS number(s): 03.67.Hk,03.65.Ud, 89.70.+c

Recently Terhal and his cooperators have proposed an novel idea of quantum data hiding [1], which explores a new application for the fantastically productive quantum information theory. It is well known that quantum mechanics can keep classical and quantum bits secret in a number of different circumstances. In some scenarios, the bits are kept secret from an eavesdropper while in others, they are kept secret from the participants themselves. The first notable example may be the quantum key distribution [2–7], which has been most near practical applications. It is the quantum generalization of the one-time pad, also know as a private quantum channel. In this case, two parties make use of shared random bits to create a secure quantum channel between them. Then they can transmit messages, which is kept secret from an eavesdropper with access to the output of the quantum channel. A second example is the quantum secret sharing [8,9], which aims to share a secret, in the form of classical or quantum bits, between many parties. Only certain prescribed combinations of the parties, known as authorized sets, are capable of fully reconstructing the secret while the other unauthorized combinations of parties can learn nothing at all about the secret, even if they act jointly on their shares.

A third example is the recent proposed quantum data hiding [1,10,11], whose purpose is also to share a secret between bi- or multi- party, but imposes a stronger security criterion than quantum secret sharing. The authorized set needs to communicate quantum data in order to get substantive information about the secret. In the Terhal's protocol of hiding bits in Bell states, the substantial information the parties could get about the secret, through any sequence of local quantum operations supplemented by unlimited two-way classical communication (LOCC), is exponentially small in the number of states used for the encoding. Various meaningful generalizations, to either hiding multiple bits or hiding quantum data, have been presented by the same workgroup in the references [10,11]. They also get two significative conclusions that perfect quantum data hiding is impossible, and the quantum data hiding with pure states is impossible, which provides the basic descriptions for the problem of quantum data hiding.

Here we analyze the practical implication of the existing quantum data hiding protocol with Bell states produced with optical downconverter. We show that the uncertainty for the produce of the Bell states with spontaneous parameter down-conversion should be taken into account, as it will cause serious trouble to the hider encoding procedure. A set of extended Bell states and a generalized Bell states analyzer are proposed to describe and analyze the possible states of two photons distributing in the two paths. Then we presented a method to combine the above uncertainty of Bell states preparation into the dating hiding procedure, when we encode the secret with the set of extended Bell states. A reasonable simple conjecture is proposed to prove the security of this modified quantum data hiding protocol. It paves the road for the experimental implementation of the quantum data hiding with present-day quantum optics.

In Terhal's quantum data hiding scheme [1], they proposed to hide bits in a series of Bell states produced with optical down-converter. When the one-bit secret $b = 1$, the hider picks at random a set of n Bell states with uniform probability, except that the number of singlets $|\Psi\rangle^-$ must be odd. The $b = 0$ protocol is the same, except that the number of singlets must be even. For each Bell state the first qubit goes to Alice and the second to Bob. It is known that the state produced with the parameter down-conversion can be written as (unnormalized)

*Electronic address: harryguo@mail.ustc.edu.cn

$$|\Sigma\rangle = (1 + p^{1/2} a_{ij}^{+} + \frac{(p^{1/2} a_{ij}^{+})^2}{2} + o(p))\,|vac\rangle \tag{1}$$

where p is the probability of producing a pair of Bell state $|\Psi\rangle_{ij}^{-} = a_{ij}^{+}\,|vac\rangle = \frac{1}{\sqrt{2}}(h_i^{\dagger} v_j^{\dagger} - v_i^{\dagger} h_j^{\dagger})\,|vac\rangle$, with h and v being the two polarization mode operators of photon. $o(p)$ represent the terms to produce more down-conversion photons whose probabilities are smaller than p^2 and $|vac\rangle$ is the vacuum state of the down-conversion photons. Obviously, the hider can not ascertain the exact producing time of the down-conversion photons and whether these photons are in the Bell state $|\Psi\rangle^{-}$. As the introducing of postselection measurements will make quantum data hiding meaningless, this uncertainty causes serious problem for the encoding of the quantum data hiding scheme. It is very difficult for the hider to pick out n Bell states and there are exactly even or odd number of singlets among these states. A device of quantum non-demolition (QND) measurement for Bell states [12] can resolve this problem. But this device needs the unavailable optical CNOT gates or single-photon sources [13].

To take into account this uncertainty for the generation of Bell states, we can modify the quantum data hiding protocol in the following way. Consider the experimental setup as Fig. 1. A pulse of ultraviolet (UV) light passing through a nonlinear crystal creates the ancillary pair of entangled photons in paths 1 and 2. After retroflection during its second passage through the crystal, the ultraviolet pulse can create another pair of photons in paths 3 and 4. In view of the uncertainty of the parameter down-conversion, the state of photon in the paths 1, 2, 3 and 4 can written as the following (unnormalized)

$$\begin{aligned} |\Xi\rangle &= (1 + p^{1/2} a_{12}^{+} + \frac{(p^{1/2} a_{12}^{+})^2}{2} + o(p)) \otimes (1 + p^{1/2} a_{34}^{+} + \frac{(p^{1/2} a_{34}^{+})^2}{2} + o(p))\,|vac\rangle \\ &= (1 + p^{1/2}(a_{12}^{+} + a_{34}^{+}) + p(a_{12}^{+} a_{34}^{+} + \frac{(a_{12}^{+})^2}{2} + \frac{(a_{34}^{+})^2}{2}) + o(p))\,|vac\rangle\,. \end{aligned} \tag{2}$$

where $a_{ij}^{+} = \frac{1}{\sqrt{2}}(h_i^{\dagger} v_j^{\dagger} - v_i^{\dagger} h_j^{\dagger})$ is creation operator for the singlets state $|\Psi\rangle^{-}$ and $|vac\rangle$ is the vacuum state of the four paths. Then we have a probability of p^2 to get four photons in the four paths 1, 2, 3 and 4 which are in the state (unnormalized):

$$|\Theta\rangle = (a_{12}^{+} a_{34}^{+} + \frac{(a_{12}^{+})^2}{2} + \frac{(a_{34}^{+})^2}{2})\,|vac\rangle\,. \tag{3}$$

It can be also written as (unnormalized)

$$\begin{aligned} |\Theta\rangle &= |\Phi\rangle_{13}^{+}\,|\Phi\rangle_{24}^{+} - |\Phi\rangle_{13}^{-}\,|\Phi\rangle_{24}^{-} - |\Psi\rangle_{13}^{+}\,|\Psi\rangle_{24}^{+} + |\Psi\rangle_{13}^{-}\,|\Psi\rangle_{24}^{-} \\ &\quad + |\Gamma\rangle_{13}^{+}\,|\Upsilon\rangle_{24}^{+} + |\Gamma\rangle_{13}^{-}\,|\Upsilon\rangle_{24}^{-} + |\Upsilon\rangle_{13}^{+}\,|\Gamma\rangle_{24}^{+} + |\Upsilon\rangle_{13}^{-}\,|\Gamma\rangle_{24}^{-} - |\Omega\rangle_{13}^{+}\,|\Omega\rangle_{24}^{+} - |\Omega\rangle_{13}^{-}\,|\Omega\rangle_{24}^{-}\,. \end{aligned} \tag{4}$$

Here $|\Phi\rangle_{ij}^{\pm} = \frac{1}{\sqrt{2}}(h_i^{\dagger} h_j^{\dagger} \pm v_i^{\dagger} v_j^{\dagger})\,|vac\rangle$ and $|\Psi\rangle_{ij}^{\pm} = \frac{1}{\sqrt{2}}(h_i^{\dagger} v_j^{\dagger} \pm v_i^{\dagger} h_j^{\dagger})\,|vac\rangle$ are the common four Bell states, which constitute a set of complete bases in the Hilbert space $H1$ where there is one photon in each of two paths i and j. The states $|\Gamma\rangle_{ij}^{\pm} = \frac{1}{2}(h_i^{\dagger} h_i^{\dagger} \pm v_j^{\dagger} v_j^{\dagger})\,|vac\rangle$, $|\Upsilon\rangle_{ij}^{\pm} = \frac{1}{2}(v_i^{\dagger} v_i^{\dagger} \pm h_j^{\dagger} h_j^{\dagger})\,|vac\rangle$ and $|\Omega\rangle_{ij}^{\pm} = \frac{1}{\sqrt{2}}(h_i^{\dagger} v_i^{\dagger} \pm h_j^{\dagger} v_j^{\dagger})\,|vac\rangle$ correspond to the case that two photons exist in one path and no photon in another path. Those six states can also be regarded as a set of complete generalized Bell bases in the Hilbert space $H2$ where two photons concentrate in one path. Then there are ten general Bell states involving two photons and two paths, which respectively belong to two sets of bases. Obviously those two set of bases lie in two different Hilbert space $H1$ and $H2$.

In the present modified quantum data hiding protocol, the hider can firstly measure the photons from the paths 1 and 3 with a optical setup as shown in the Fig. 1 [15]. When there are coincidence clicks between the two same mode detectors D_V^u and D_V^d (or D_H^u and D_H^d), the two photons in paths 1 and 3 are measured in either the state $|\Phi\rangle_{13}^{+}$ or the state $|\Omega\rangle_{13}^{+}$. And then the two photons in paths 2 and 4 are collapsed into the state $|\Phi\rangle_{24}^{+}$ and the state $|\Omega\rangle_{24}^{+}$ respectively. Similarly, when there are coincidence clicks between two different mode detectors D_H^u and D_V^d (or D_V^u and D_H^d), the two photons in paths 1 and 3 are measured in either the state $|\Phi\rangle_{13}^{-}$ or the state $|\Omega\rangle_{13}^{-}$. And then the two photons in paths 2 and 4 are collapsed into the state $|\Phi\rangle_{24}^{-}$ or the state $|\Omega\rangle_{24}^{-}$. Analogous to the existing Bell states analyzer with linear optics, the general Bell analyzer (GBA) in the Fig.1 can separate the ten general Bell states into three classes: $|\Phi\rangle_{ij}^{+}$ and $|\Omega\rangle_{ij}^{+}$ as the first class, $|\Phi\rangle_{ij}^{-}$ and $|\Omega\rangle_{ij}^{-}$ as the second class, and the others as the third class.

Conditional on the detecting of the photons in path 1 and 3, the hider can conveniently picks up n pairs of such general Bell states of the above three classes in paths 2 and 4. When the one-bit secret $b = 1$, she picks odd number

of the first class states (can be either $|\Phi\rangle_{ij}^{+}$ or $|\Omega\rangle_{ij}^{+}$) among these n pairs states picked at random. For the case $b = 0$, she picks even number of the first class states in those n pairs general Bell states. This encoding procedure is very straightforward and effortless. And the uncertainty caused by the parameter down conversion has been ingeniously combined into the encoding states.

Then the photons in paths 2 and 4 are sent to the shares Alice and Bob respectively. For the completely unlocking of the secret, a quantum channel between Alice and Bob is opened up and Alice's photons are sent to Bob. So Bob can measure these photons with the same general Bell states analyzer (GBA) as the hider has used. Alice and Bob simply count the number of the first class states measured (the number of the coincidence clicks between two same mode detectors), and compute the parity to get the secret.

The rigorous proof for the security of the present quantum data hiding protocol with ten generalized Bell states is involuted and will be present otherwhere [16]. Assume there are m pairs of states from the set $S1 = \{|\Phi\rangle^{\pm}, |\Psi\rangle^{\pm}\}$ and $(n-m)$ pairs of states from the set $S2 = \{|\Gamma\rangle^{\pm}, |\Upsilon\rangle^{\pm}, |\Omega\rangle^{\pm}\}$ among the n pairs of encoded states. As the states of the two sets $S1$ and $S2$ lie in two different Hilbert space $H1$ and $H2$, and respectively represent the cases the two photons distribute in two paths and concentrate in one path, we reasonably conjecture that the parity of the total number of the states $|\Phi\rangle^{+}$ and $|\Omega\rangle^{+}$ in the tensor product of n general Bell states of the above two sets cannot be decoded better than to combine the results from the decoding of the parity $b1$ of the number of the state $|\Phi\rangle^{+}$ in the tensor product of m pairs of $S1$ set states, and decoding of the parity $b2$ of the number of the state $|\Omega\rangle^{+}$ in the tensor product of $(n-m)$ pairs of $S2$ set states. In theory, the shares can do any measurement on the photons, such as having quantum non-demolition photon-Fock-state-filter, to separate two sets of states. Then with local operations and classical communication (LOCC), Alice and Bob can decode the parity $b2$ by counting the exact number of the state $|\Omega\rangle^{+}$ among the $(n-m)$ pair $S2$ set states. But the mutual information $I(b1 : M)$ [17] the shares can get about the parity b1 with any LOCC measurement M on the m pairs $S1$ states is bounded by $\delta H(b1)$ [1], where $\delta = 1/2^{m-1}$ and $H(B1)$ is the Shannon information of the hidden bit. As the secret $b = b1 \oplus b2$, with $\oplus$ being the addition modulo two, the mutual information the shares can get about the secret $I(b : M)$ is still bounded by $\delta H(b1) = H(B1)/2^{m-1}$. Obviously, the hider has a probability of $2/5$ to prepare the two photon in path 2 and 4 in the $S1$ set states in the present quantum data hiding scheme with spontaneous parameter down-conversion. Thus the present protocol needs $5/2$ times as many pairs states as in the original quantum data hiding with Bell states to achieve the same level of security.

In conclusion, we have analyzed the practical implication of the existing quantum data hiding protocol with Bell states produced with optical downconverter. We showed that the uncertainty for the produce of the Bell states with spontaneous parameter down-conversion should be taken into account, as it will cause serious trouble to the hider encoding procedure. A set of extended Bell states and a generalized Bell states analyzer are proposed to describe and analyze the possible states of two photons distributing in the two paths. Then we presented a method to combine the above uncertainty of Bell states preparation into the dating hiding procedure, when we encode the secret with the set of extended Bell states. This greatly simplify the hider's encoding operations. An un-rigorous but reasonable proof for security of the present quantum data hiding protocol has also been proposed. It paves the road for the experimental implementation of the quantum data hiding with present-day quantum optics.

We thanks Barbara Terhal for the discuss in the security of the present protocol. This work was funded by National Fundamental Research Program(2001CB309300), National Natural Science Foundation of China, the Innovation funds from Chinese Academy of Sciences, and also by the outstanding Ph. D thesis award and the CAS's talented scientist award entitled to Luming Duan.

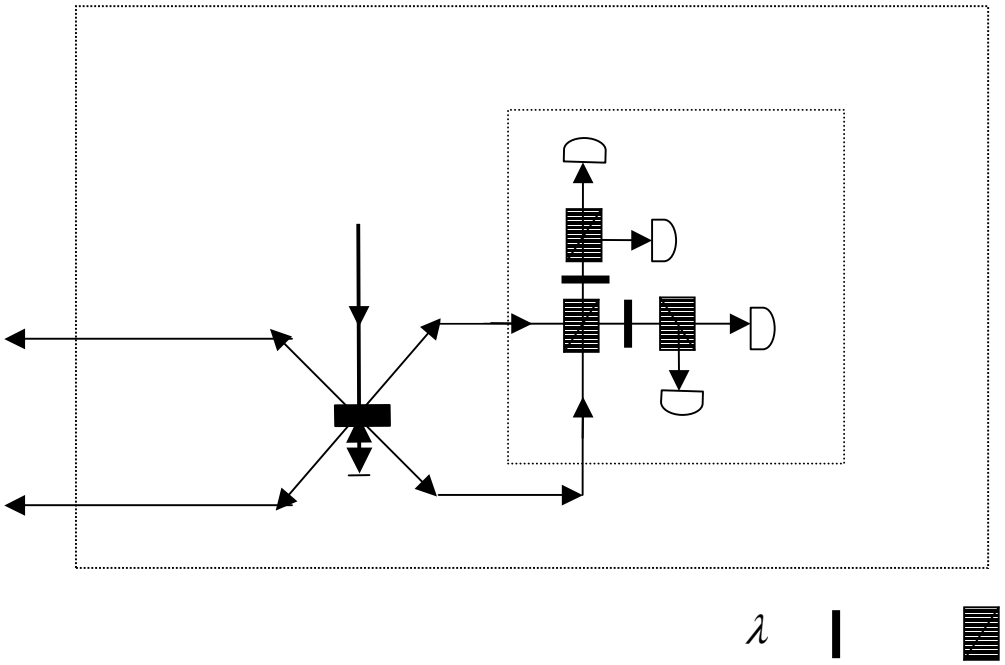
---

[1] B. M. Terhal, D. P. Divincenzo, and D. W. Leung, Phys. Rev. Lett. 86, 5807 (2001).
[2] C. H. Bennett, and G. Brassard, Advances in Cryptology: Proceedings of Ctypto84, August 1984, Springer-Verlag, p.475.
[3] C. H. Bennett, Phys. Rev. Lett. 68, 3132 (1992).
[4] A. Ekert, Phy. Rev. Lett. 67, 661 (1991).
[5] L. Goldenberg, and L. Vaidman, Phys. Rev. Lett. 75, 1239 (1995).
[6] G. P. Guo, C. F. Li, B. S. Shi, J. Li, and G. C. Guo, Phys. Rev. A 64, 042301 (2001).
[7] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. In IEEE Symposium in Foundations of Computer Science (FOCS), 547 (2000).
[8] R. Cleve, D. Gottesman, and H. K. Lo. Phys. Rev. Lett. 83, 648 (1999).

[9] G. P. Guo, and G. C. Guo to appear in Phys. Lett. A.
[10] D. P. Divincenzo, P. Hayden, and B. M. Terhal. quant-ph/0207147.
[11] D. P. Divincenzo, D. W. Leung, and B. M. Terhal. quant-ph/0103098.
[12] G. P. Guo, C. F. Li, and G. C. Guo, Phys. Lett. A 286,401 (2001).
[13] E. Knill, R. Laflamme, and G. Milburn, Nature 409, 46 (2001).
[14] G. P. Guo, and G. C. Guo quant-ph/0208071.
[15] G. P. Guo, and G. C. Guo quant-ph/0301009.
[16] G. P. Guo, and G. C. Guo in preparation.
[17] T. M. Cover and J. A. Thomas, Elements of Information Theory (Wiley, New York, 1991).

Figure Captions:

Figure1: The schematic set-up for the perfect quantum data hiding protocol modified from the hiding with Bell states. A pulse of ultraviolet (UV) light passing through a nonlinear crystal creates the ancillary pair of entangled photons in paths 1 and 2. After retroflection during its second passage through the crystal, the ultraviolet pulse can create another pair of photons in paths 3 and 4. Then there is probability of p^2 to have four photons in the four paths 1, 2, 3 and 4. The $\lambda/2$ plates are used to implement Hardmard operations, which transform the h mode photon into $h - v$ and v mode into $h + v$. The hider measures the photons from the path 1 and 3 with an general Bell states analyzer(GBA) [14] and then picks up n pairs of states to encode secret, whose photons in paths 2 and 4 are sent to Alice and Bob respectively. In the secret unlock procedure, Alice and Bob can measure the photons from paths 2 and 4 with the same analyzer(GBA).


λ